Journal of Number Theory 130 (2010) 1737–1749

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A binary linear recurrence sequence of composite numbers

Artūras Dubickas *, Aivaras Novikas, Jonas Šiurys

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania

ARTICLE INFO

Article history:
Received 22 March 2010
Available online 15 May 2010
Communicated by Ronald Graham

MSC:
11B37
11A07
11Y55

Keywords:
Binary recurrence
Composite number
Covering systems
Divisibility sequence

ABSTRACT

Let $(a,b)\in\mathbb{Z}^2$, where $b\neq 0$ and $(a,b)\neq(\pm 2,-1)$. We prove that then there exist two positive relatively prime composite integers x_1, x_2 such that the sequence given by $x_{n+1}=ax_n+bx_{n-1}$, $n=2,3,\ldots$, consists of composite terms only, i.e., $|x_n|$ is a composite integer for each $n\in\mathbb{N}$. In the proof of this result we use certain covering systems, divisibility sequences and, for some special pairs $(a,\pm 1)$, computer calculations. The paper is motivated by a result of Graham who proved this theorem in the special case of the Fibonacci-like sequence, where $(a,b)=(1,1)$.

1. Introduction

The main result of this paper is the following:

Theorem 1. *Let $(a,b)\in\mathbb{Z}^2$ and let $(x_n)_{n=1}^{\infty}$ be a sequence given by some initial values x_1, x_2 and the binary linear recurrence*

$$x_{n+1}=ax_n+bx_{n-1} \tag{1}$$

for $n=2,3,4,\ldots$. Suppose that $b\neq 0$ and $(a,b)\neq(2,-1),(-2,-1)$. Then there exist two relatively prime positive integers x_1, x_2 such that $|x_n|$ is a composite integer for each $n\in\mathbb{N}$.

* Corresponding author.
E-mail addresses: arturas.dubickas@mif.vu.lt (A. Dubickas), aivaras.novikas@mif.vu.lt (A. Novikas), jonas.siurys@gmail.com (J. Šiurys).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.03.015

To avoid confusion with zero and one, we call a non-negative integer n a composite number if $n \neq 0, 1$ and n is not a prime number. The question of determining prime and composite numbers in a given integer sequence is an old one. For instance, it is not known if there are infinitely many primes of the form n^2+1, $n \in \mathbb{N}$, and if there are infinitely many primes in the Fibonacci sequence F_n, $n \in \mathbb{N}$, given by $F_1 = F_2 = 1$ and the recurrence relation $F_{n+1} = F_n + F_{n-1}$ for $n \geqslant 2$. Although almost all positive integers are composite, for some quite natural sequences, for example, $[r^n]$, where $r > 1$ is a rational non-integer number and n runs through the set of positive integers $\mathbb{N}$, it is not even known if they contain infinitely many composite numbers or not (see Problem E19 in [6]). The latter question is only settled for $r = 3/2$, $r = 4/3$ in [4] and for $r = 5/4$ in [3]. See also [1,2] for some related problems.

The main motivation of this paper is a result of Graham [5] who found two relatively prime positive integers x_1, x_2 such that the sequence

$$x_{n+1} = x_n + x_{n-1},$$

$n = 2, 3, 4, \ldots$, contains only composite numbers, i.e., x_n is composite for each $n \in \mathbb{N}$. Graham's pair (x_1, x_2) was

$$(331635635998274737472200656430763, 151002891108840197118959030549878 5).$$

Knuth [8] found the smaller pair

$$(x_1, x_2) = (62638280004239857, 49463435743205655).$$

Wilf [11] slightly refined Knuth's computation and found the pair

$$(x_1, x_2) = (20615674205555510, 3794765361567513).$$

This was further reduced by Nicol [9] to

$$(x_1, x_2) = (407389224418, 76343678551).$$

Currently, the "smallest" known such pair (in the sense that $x_1 + x_2$ is the smallest positive integer or $\max(x_1, x_2)$ is the smallest positive integer) is due to Vsemirnov [10]

$$(x_1, x_2) = (106276436867, 35256392432). \tag{2}$$

All these results are based on the fact that the Fibonacci sequence is a *divisibility sequence,* i.e., $F_n | F_m$ whenever $n|m$, and on finding a *covering system* $r_i \pmod{m_i}$, $i = 1, \ldots, t$, with the property that there exist distinct prime numbers p_i such that $p_i | F_{m_i}$ for $i = 1, \ldots, t$. See Section 4 for more details. We shall also use Graham's idea of finding an appropriate covering system for $|b| = 1$ and Vsemirnov's pair (2) in order to treat some special cases with $|b| = 1$ in our proof.

Let $\alpha := (a + \sqrt{D})/2$ and $\beta := (a - \sqrt{D})/2$, where $\sqrt{D}$ is defined as $i\sqrt{-D}$ for $D < 0$, be two roots of the characteristic equation

$$x^2 - ax - b = (x - \alpha)(x - \beta) = 0 \tag{3}$$

with discriminant

$$D := (\alpha - \beta)^2 = a^2 + 4b. \tag{4}$$

By (3) and (4), we have $\alpha-\beta=\sqrt{D}$, $\alpha\beta=-b$ and $\alpha+\beta=a$. It is easily seen that, for each $n\in\mathbb{N}$, the nth term of the sequence $(x_n)_{n=1}^{\infty}$ defined in (1) is given by

$$x_n=\frac{-x_1\beta+x_2}{\alpha-\beta}\alpha^{n-1}+\frac{x_1\alpha-x_2}{\alpha-\beta}\beta^{n-1} \tag{5}$$

provided that $\alpha\neq\beta$, i.e., $D\neq 0$. For $\alpha=\beta$, i.e., $D=0$ we have

$$x_n=\bigl(2x_1-x_2\alpha^{-1}+n\bigl(x_2\alpha^{-1}-x_1\bigr)\bigr)\alpha^{n-1} \tag{6}$$

for each $n\in\mathbb{N}$.

Our plan of the proof of Theorem 1 can be described as follows. In Section 2 we shall examine the following three cases: (i) $D=0$; (ii) $a=0$; (iii) $b=-1$, $|a|\leqslant 2$. Also, in Section 2 we show that the condition of the theorem $(a,b)\neq(\pm 2,-1)$ is necessary.

In case $|b|\geqslant 2$ we shall take x_2 divisible by $|b|$. Then, by (1), x_3 and so, by induction, all x_n, where $n\geqslant 2$, are divisible by $|b|$. The main difficulty is to show that x_1 can be chosen so that $x_n\neq 0,b,-b$ for each $n\geqslant 3$, so that $|x_n|$ is composite. This case, $|b|\geqslant 2$, will be examined in Section 3. Finally, in Section 4 we shall describe the method of covering systems and prove the theorem for $|b|=1$.

It would be of interest to extend Theorem 1 to linear recurrence sequences of order d, where $d\geqslant 3$. For which $(a_1,\dots,a_d)\in\mathbb{Z}^d$, where $a_d\neq 0$, one can choose d integers $x_1,\dots,x_d$ satisfying $\gcd(x_1,\dots,x_d)=1$ such that the sequence

$$x_{n+d}=a_1x_{n+d-1}+a_2x_{n+d-2}+\cdots+a_dx_n,\quad n=1,2,3,\dots,$$

contains only composite numbers, i.e., $|x_n|$ is a composite integer for each $n\geqslant 1$?

It seems likely that the complete answer to this question is out of reach. Firstly, for most linear recurrences of order d, there are no divisibility sequences satisfying them. See, e.g., Theorem IV in the paper of Hall [7] for one of the first results of this kind for $d=3$. So, using the methods of this paper, one will not be able to deal with the cases, where, e.g., $a_i\in\{-1,0,1\}$ for each $i=1,\dots,d$ and the characteristic polynomial of the linear recurrence is irreducible. Secondly, and more importantly, there are no methods that would allow us to show that the cases, where the characteristic polynomial

$$x^d-a_1x^{d-1}-a_2x^{d-2}-\cdots-a_d$$

is $(x+1)^d$ or $(x-1)^d$, are exceptional. Already for $d=3$ and, say, $(a_1,a_2,a_3)=(3,-3,1)$ one gets a problem on prime values of a quadratic polynomial $\mathbb{Z}\mapsto\mathbb{Z}$ at non-negative integer points which is completely out of reach.

2. Several simple special cases

In this section we shall consider three special cases: (i) $D=0$; (ii) $a=0$; (iii) $b=-1$, $|a|\leqslant 2$.

Case (i). Since $D=a^2+4b=0$, the solution of the linear recurrence (1) is given by (6). Note that $a=2\alpha$ and $b=-\alpha^2$. So α is a nonzero integer. We shall split the proof into two cases $|\alpha|\geqslant 2$ and $|\alpha|=1$.

In the first case, $|\alpha|\geqslant 2$, let us take two distinct primes p,q satisfying $p,q>|\alpha|$ and select $x_1:=p^2$, $x_2:=|\alpha|q^2$. Then x_1, x_2 are composite and $\gcd(x_1,x_2)=1$. Furthermore, writing $|\alpha|=\alpha\varepsilon$, where $\varepsilon=\pm 1$, by (6), we obtain

$$x_n=\bigl(2p^2-q^2\varepsilon+n\bigl(q^2\varepsilon-p^2\bigr)\bigr)\alpha^{n-1}$$

for each $n \geqslant 1$. Clearly, $|x_n|$ is divisible by $|\alpha^2| = |b| \geqslant 4$ for $n \geqslant 3$, so $|x_n|$ is composite for each $n \in \mathbb{N}$, unless

$$2p^2 - q^2\varepsilon + n\big(q^2\varepsilon - p^2\big) = 0$$

for some n. But this equality cannot hold for $n \in \mathbb{N}$. Indeed, if $\varepsilon = -1$, then

$$n = \frac{2p^2 + q^2}{p^2 + q^2} = 1 + \frac{p^2}{p^2 + q^2}$$

is greater than 1 and smaller than 2, a contradiction. If $\varepsilon = 1$, then $(n-1)q^2 = (n-2)p^2$ implies $n - 1 = \ell p^2$ and $n - 2 = \ell q^2$ with $\ell \in \mathbb{Z}$. Hence $1 = (n-1) - (n-2) = \ell(p^2 - q^2)$, which is impossible, because $p, q > |\alpha| \geqslant 2$ yields $|p^2 - q^2| \geqslant |5^2 - 3^2| = 16 > 1$.

Suppose next that $\alpha = \pm 1$. Then $b = -\alpha^2 = -1$ and $a = \pm 2$. This case is not allowed by the condition of the theorem. Moreover, it is easy to see that in this case the sequence $(|x_n|)_{n=1}^{\infty}$, where x_1, x_2 are composite and $\gcd(x_1, x_2) = 1$, contains infinitely many prime numbers. Indeed, by (6),

$$x_n = \big(2x_1 - x_2\varepsilon + n(x_2\varepsilon - x_1)\big)\varepsilon^{n-1}$$

for each $n \geqslant 1$ and $\varepsilon = \pm 1$. Since x_1 and x_2 are relatively prime positive composite integers, we must have $u := 2x_1 - x_2\varepsilon \neq 0$ and $v := x_2\varepsilon - x_1 \neq 0$. Moreover, $\gcd(x_1, x_2) = 1$ implies $\gcd(u, v) = 1$. So, by Dirichlet's theorem on prime numbers in arithmetic progressions, we conclude that $|x_n| = |vn + u|$ is a prime number for infinitely many $n \in \mathbb{N}$. This not only completes the proof of Theorem 1 in the case $D = 0$, but also shows that the condition $(a, b) \neq (\pm 2, -1)$ is necessary.

Case (ii). For $a = 0$, we have $x_{n+1} = bx_{n-1}$ for $n \geqslant 2$. Let $p, q > |b|$ be two distinct primes. Selecting $x_1 := p^2$ and $x_2 := q^2$, we have $\gcd(x_1, x_2) = 1$. Furthermore, $x_{2k-1} = p^2 b^{k-1}$ and $x_{2k} = q^2 b^{k-1}$ for each $k \geqslant 1$, so $|x_n|$ is composite for every $n \in \mathbb{N}$.

Case (iii). The cases $(a, b) = (\pm 2, -1)$ and $(a, b) = (0, -1)$ are already covered by Case (i) and Case (ii), respectively. If $(a, b) = (-1, -1)$ the recurrence sequence $x_{n+1} = -x_n - x_{n-1}$ satisfying the condition of the theorem is, for example, the following periodic sequence:

$$9, 16, -25, 9, 16, -25, 9, 16, -25, \ldots.$$

For $(a, b) = (1, -1)$, we have the recurrence $x_{n+1} = x_n - x_{n-1}$. Now, the periodic sequence

$$16, 25, 9, -16, -25, -9, 16, 25, 9, -16, -25, -9, \ldots$$

satisfies the conditions of the theorem.

3. The case $|b| \geqslant 2$

Lemma 2. *Let d and ℓ be two positive integers. Then there is a positive integer c and three distinct odd prime numbers p, q, r such that pqr divides $d + c^2$ and $\gcd(pqr, \ell c) = 1$.*

Proof. Given $h \in \mathbb{Z}$ and a prime number p, let $(\frac{h}{p})$ be the Legendre symbol. Take three distinct prime numbers p, q, r greater than $\max(d, \ell)$ such that

$$\left(\frac{-d}{p}\right) = \left(\frac{-d}{q}\right) = \left(\frac{-d}{r}\right) = 1.$$

(For example, one can take the prime numbers p, q, r in the arithmetic progression $4kd + 1$, $k = 1, 2, \ldots$.) Then there are three positive integers c_1, c_2, c_3 such that $c_1^2 \equiv -d \pmod{p}$, $c_2^2 \equiv -d \pmod{q}$, $c_3^2 \equiv -d \pmod{r}$. By the Chinese remainder theorem, there is a positive integer c such that $c \equiv c_1 \pmod{p}$, $c \equiv c_2 \pmod{q}$, $c \equiv c_3 \pmod{r}$. Then $c^2 \equiv -d \pmod{pqr}$. This proves that pqr divides $d + c^2$.

Since $p, q, r > \ell$, none of the primes p, q, r divides ℓ. Assume that $p|c$. Then $p|(d + c^2)$ implies $p|d$, which is impossible, because $p > d$. By the same argument, q and r do not divide c. This completes the proof of $\gcd(pqr, \ell c) = 1$. □

Lemma 3. *Let u_i, v_i, $i = 1, 2, \ldots, p-1$, and s be the elements of the field $\mathbb{F}_p$, where p is a prime number. Assume that for each i at least one of u_i, v_i is nonzero. Then there exist $u, v \in \mathbb{F}_p$ such that at least one of u, v is nonzero and $uu_i + vv_i \neq s$ for each $i = 1, \ldots, p-1$.*

Proof. Fix an index i in the range $1 \leqslant i \leqslant p-1$. We claim that there are exactly p pairs $(u, v) \in \mathbb{F}_p^2$ for which

$$uu_i + vv_i = s. \tag{7}$$

Indeed, if $u_i = 0$, then $v_i \neq 0$ and (u, sv_i^*), where $u \in \mathbb{F}_p$ and v_i^* is the inverse element of v_i in $\mathbb{F}_p$, are the solutions of (7). By the same argument, (7) has p solutions if $v_i = 0$. Finally, if $u_i \neq 0$ and $v_i \neq 0$, then we can take any $u \in \mathbb{F}_p$ and the linear equation (7) has a unique solution in v. This proves the claim.

As i runs through $1, \ldots, p-1$, we have $p-1$ Eqs. (7) which all together have at most $p(p-1)$ distinct solutions $(u, v) \in \mathbb{F}_p^2$. But $\mathbb{F}_p^2$ consists of the pair $(0, 0)$ and $p^2 - 1$ pairs (u, v) with at least one u, v nonzero. Since $p^2 - 1 > p(p-1)$, there exists a pair $(u, v) \in \mathbb{F}_p^2$ as required, namely, $u \neq 0$ or $v \neq 0$ and $uu_i + vv_i \neq s$ for each $i = 1, \ldots, p-1$. □

Lemma 4. *Let $c > 0$, $D < 0$ and a be three integers. Suppose that p is an odd prime number which divides $-D + c^2$ but does not divide c. Then the sequence of rational integers*

$$s_n := \frac{(a + \sqrt{D})^n - (a - \sqrt{D})^n}{2\sqrt{D}}, \tag{8}$$

$n = 1, 2, 3, \ldots$, is purely periodic modulo p with period $p - 1$. Also, no two consecutive elements of the sequence $(s_n)_{n=1}^{\infty}$ can be zeros modulo p.

Proof. By (8), we have

$$s_n = \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1} D^k,$$

where 0^0 is defined as 1. Since $D \equiv c^2 \pmod{p}$ and

$$\sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1} c^{2k} = \frac{(a+c)^n - (a-c)^n}{2c},$$

we find that

$$s_n \equiv \frac{(a+c)^n - (a-c)^n}{2c} \pmod{p}. \tag{9}$$

Since p and $2c$ are relatively prime, it remains to show that, for each $n \geqslant 1$, we have

$$(a+c)^{n+p-1} - (a-c)^{n+p-1} \equiv (a+c)^n - (a-c)^n \pmod{p}.$$

Indeed, by Fermat's little theorem, p divides both the numbers $(a+c)^{n+p-1} - (a+c)^n = (a+c)^n \times ((a+c)^{p-1} - 1)$ and $(a-c)^{n+p-1} - (a-c)^n$, so p also divides their difference. This proves the periodicity.

For the second statement of the lemma, assume that $s_n \equiv 0 \pmod{p}$ and $s_{n+1} \equiv 0 \pmod{p}$ for some $n \in \mathbb{N}$. Then, by (9), $(a+c)^n \equiv (a-c)^n \pmod{p}$ and $(a+c)^{n+1} \equiv (a-c)^{n+1} \pmod{p}$. If $a \equiv c \pmod{p}$ then $a \equiv -c \pmod{p}$, so p divides $2c$, which is not the case by the condition of the lemma. Similarly, a and $-c$ modulo p are distinct. Hence, from

$$(a-c)^{n+1} \equiv (a+c)^{n+1} \equiv (a+c)^n(a+c) \equiv (a-c)^n(a+c) \pmod{p},$$

we find that $a+c \equiv a-c \pmod{p}$. Once again this yields $p|2c$, a contradiction. □

Lemma 5. *Let $(x_n)_{n=1}^{\infty}$ be a sequence of integers given by* (1)*, $D = a^2 + 4b \neq 0$, $b \neq 0$, and let δ be a fixed real number. Then $x_{n+1} = \delta b$ for some $n \geqslant 2$ if and only if*

$$x_1 \frac{s_{n-1}}{2^{n-2}} + \frac{x_2}{b} \frac{s_n}{2^{n-1}} = \delta,$$

where s_n is given by (8)*.*

Proof. The roots α and β of the characteristic equation (3) are distinct, so, by (5) and $\alpha - \beta = \sqrt{D}$, we have

$$x_{n+1}\sqrt{D} = (-x_1\beta + x_2)\alpha^n + (x_1\alpha - x_2)\beta^n \tag{10}$$

for each $n \geqslant 0$. Since $2\alpha = a + \sqrt{D}$ and $2\beta = a - \sqrt{D}$, using (8), we find that $\alpha^n - \beta^n = 2^{1-n}\sqrt{D}s_n$. Since $\alpha\beta = -b$, equality (10) yields

$$x_{n+1}\sqrt{D} = x_2\big(\alpha^n - \beta^n\big) - x_1\alpha\beta\big(\alpha^{n-1} - \beta^{n-1}\big) = x_2 2^{1-n} s_n\sqrt{D} + x_1 b 2^{2-n} s_{n-1}\sqrt{D}.$$

Hence $x_{n+1} = x_1 b 2^{2-n} s_{n-1} + x_2 2^{1-n} s_n$, because $D \neq 0$. It follows that equality $x_{n+1} = \delta b$ is equivalent to

$$\delta = x_1 \frac{s_{n-1}}{2^{n-2}} + \frac{x_2}{b} \frac{s_n}{2^{n-1}},$$

as claimed. □

Lemma 6. *Let $(x_n)_{n=1}^{\infty}$ be a sequence of integers given by* (1)*, where $a \neq 0$ and $D > 0$. Then, for each $K > 0$ and each x_1, there is a constant $\lambda(K, \alpha, \beta, x_1) > 0$ such that by selecting the two first terms of the sequence* (1) *as x_1 and $x_2 > \lambda(K, \alpha, \beta, x_1)$ we have $|x_n| > K$ for each $n \geqslant 2$.*

Proof. Since $D > 0$ and $a = \alpha + \beta \neq 0$, we have $|\alpha| \neq |\beta|$. Suppose that $|\alpha| > |\beta|$. (The proof in the case $|\alpha| < |\beta|$ is the same.) From $\alpha\beta = -b$, we obtain $|\alpha| > \sqrt{|b|} \geqslant 1$. Hence, by (10), using several times the triangle inequality, for $n \geqslant 1$, we obtain

$$|x_{n+1}|\sqrt{D} \geqslant \big|(-x_1\beta + x_2)\alpha^n\big| - \big|(x_1\alpha - x_2)\beta^n\big| = |bx_1 + x_2\alpha||\alpha|^{n-1} - |-bx_1 - x_2\beta||\beta|^{n-1}$$
$$\geqslant \big(|bx_1 + x_2\alpha| - |bx_1 + x_2\beta|\big)|\alpha|^{n-1} \geqslant \big(|bx_1 + x_2\alpha| - |bx_1 + x_2\beta|\big)|\alpha|^{n-1}$$
$$\geqslant \big(|x_2\alpha| - |bx_1| - |bx_1| - |x_2||\beta|\big)|\alpha|^{n-1} = \big(|x_2|\big(|\alpha| - |\beta|\big) - 2|bx_1|\big)|\alpha|^{n-1}.$$

Since $|\alpha|^{n-1} \geqslant 1$ for $n \geqslant 1$, the last expression is greater than $K\sqrt{D}$ provided that $|x_2|(|\alpha| - |\beta|) > 2|bx_1| + K\sqrt{D}$. So the lemma holds with

$$\lambda(K, \alpha, \beta, x_1) := \frac{2|bx_1| + K\sqrt{D}}{|\alpha| - |\beta|} \tag{11}$$

when $|\alpha| > |\beta|$. Evidently, the constants b, D appearing in the right-hand side of (11) depend on α, β too, because $b = -\alpha\beta$ and $D = a^2 + 4b = (\alpha - \beta)^2$, by (3), (4). □

Lemma 7. *Let $a_1 \geqslant 0$ and $b_1, b_2 \geqslant 1$ be integers such that no prime number p divides the three numbers a_1, b_1, b_2. Then, for each $K > 0$, there exists an integer $k_1 > K$ such that $b_1k_1 + a_1$ is a composite integer relatively prime to b_2.*

Proof. The lemma is trivial if $a_1 = 0$. Assume that $a_1 \geqslant 1$. Set $t := \gcd(b_1, a_1)$. By the condition of the lemma, t is relatively prime to b_2. By Dirichlet's theorem about prime numbers in arithmetic progressions, there is a $t_1 \in \mathbb{N}$ such that $(b_1/t)t_1 + a_1/t$ is a prime number greater than b_2. Then $b_1t_1 + a_1 = t((b_1/t)t_1 + a_1/t)$ is relatively prime to b_2. This implies that, for any $s \in \mathbb{N}$, the number

$$b_1b_2s + b_1t_1 + a_1 = b_1(b_2s + t_1) + a_1$$

is relatively prime to b_2. Of course, there are infinitely many $s \in \mathbb{N}$ for which the number $b_1b_2s + b_1t_1 + a_1$ is composite. It remains to take one of those $s \in \mathbb{N}$ for which $k_1 := b_2s + t_1 > K$. □

We begin the proof of the theorem for $|b| \geqslant 2$ from the more difficult case when the discriminant $D = a^2 + 4b$ is negative. Let us apply Lemma 2 to $d := -D$ and $\ell := |b|$. Then, by Lemma 2, there exist a positive integer c and three distinct odd primes p, q, r such that pqr divides $-D + c^2$ and

$$\gcd\big(pqr, |b|c\big) = 1. \tag{12}$$

Our aim is to choose two composite relatively prime positive integers x_1, x_2 so that $|b|$ divides x_2 and $x_{n+1} \notin \{0, b, -b\}$ for each $n \geqslant 2$. Then $|x_1| = x_1$ and $|x_2| = x_2$ are composite. Also, using (1), by induction on n we see that $|b|$ divides x_{n+1} for each $n \geqslant 1$. Since $x_n \notin \{0, b, -b\}$ for $n \geqslant 3$ and $|b|$ divides x_n for $n \geqslant 2$, we must have $|x_n| > |b|$ for each $n \geqslant 3$. Hence $|x_n|$ is a composite integer for every $n \geqslant 3$ too.

For a contradiction, assume that, for some $n \geqslant 1$, $x_{n+2} = \delta b$ with $\delta \in \{0, 1, -1\}$. Then, by Lemma 5, we have

$$x_1\frac{s_n}{2^{n-1}} + x_2'\frac{s_{n+1}}{2^n} = \delta, \tag{13}$$

where $x_2' := x_2/b$ and $n \in \mathbb{N}$. Firstly, let us choose x_1, x_2' modulo p so that

$$2x_1s_n + x_2's_{n+1} \neq 0, \quad n \in \mathbb{N}. \tag{14}$$

This is possible by combining Lemma 4 with Lemma 3. Indeed, by Lemma 4, the sequence $s_n \pmod p$, $n = 1, 2, 3, \ldots$, is purely periodic with period $p - 1$. So, by Lemma 3 applied to the

pairs $(2s_1, s_2), (2s_2, s_3), \dots, (2s_{p-1}, s_p) \in \mathbb{F}_p^2$ and $s = 0$, we conclude that there are $x_1, x_2' \in \mathbb{F}_p$, not both zeros in $\mathbb{F}_p$, such that (14) holds.

Next, we shall choose $x_1, x_2' \in \mathbb{F}_q$ so that

$$2x_1 s_n + x_2' s_{n+1} \neq 2^n, \quad n \in \mathbb{N}, \tag{15}$$

in $\mathbb{F}_q$. As above, by Lemma 4, the sequence $s_n 2^{1-n} \pmod q$, $n = 1, 2, 3, \dots$, where 2^{1-n} is the inverse of 2^{n-1} in $\mathbb{F}_q$, is purely periodic with period $q-1$. By Lemma 3 applied to the pairs $(s_1, 2^{-1}s_2), (s_2 2^{-1}, s_3 2^{-2}), \dots, (s_{q-1}2^{-(q-2)}, s_q 2^{-(q-1)}) \in \mathbb{F}_q^2$ and $s = 1$, we conclude that there are $x_1, x_2' \in \mathbb{F}_q$, not both zeros, such that (15) holds. By the same argument, there are $x_1, x_2' \in \mathbb{F}_r$, not both zeros, such that

$$2x_1 s_n + x_2' s_{n+1} \neq -2^n, \quad n \in \mathbb{N}, \tag{16}$$

in $\mathbb{F}_r$.

By the Chinese remainder theorem, combining (14), (15), (16), we see that there exist two congruence classes $a_1 \pmod{pqr}$ and $a_2 \pmod{pqr}$ such that for any integers x_1 and x_2' that belong to the first and the second class, respectively, equality (13) does not hold for $n \in \mathbb{N}$. Furthermore, by Lemma 3, each prime number p, q, r divides at most one of the integers a_1, a_2. It remains to select $k_1, k_2 \in \mathbb{Z}$ so that $x_1 = pqrk_1 + a_1$ and $x_2 = bx_2' = b(pqrk_2 + a_2)$ are two composite relatively prime positive integers. Take $k_2 \in \mathbb{Z}$ such that $|pqrk_2 + a_2| > 1$, $bk_2 > 0$. Then $x_2 > 0$ is a composite number. Furthermore, no prime number divides the three numbers pqr, a_1 and x_2, because the primes p, q, r do not divide $|b|$, by (12), and if, say, $p|a_1$ then p does not divide $pqrk_2 + a_2$. Hence, by Lemma 7 applied to the triplet $b_1 := pqr$, a_1, $b_2 := x_2$, we may select $k_1 \in \mathbb{N}$ so that $x_1 = pqrk_1 + a_1$ is a composite integer relatively prime to x_2. This proves the theorem for $|b| \geqslant 2$, $D < 0$.

The case when $D = a^2 + 4b > 0$ is easier. As above, we need to choose two composite relatively prime positive integers x_1, x_2 such that $|b|$ divides x_2 and show that this choice leads to $x_{n+1} \notin \{0, b, -b\}$ for each $n \geqslant 2$. If $|\alpha| = |\beta|$, then $\alpha = -\beta$, so $a = \alpha + \beta = 0$. This case is already settled in Section 2. Assume next that $|\alpha| \neq |\beta|$. Take $x_1 := p^2$ and $x_2 := b^2 q$, where $p, q > |b|$ are prime numbers and q is so large that $b^2 q$ is greater than the constant $\lambda(|b|, \alpha, \beta, p^2)$ given in (11). Then, by Lemma 6, $|x_{n+1}| > |b|$ for $n \geqslant 2$. This completes the proof of Theorem 1 in case $|b| \geqslant 2$.

4. Divisibility sequences, covering systems and the case $|b| = 1$

We remind the reader once again that a sequence of rational integers $(v_n)_{n=1}^{\infty}$ is called a *divisibility sequence* if v_r divides v_s whenever r divides s. Assume that the roots α, β of the characteristic equation (3) are distinct $\alpha \neq \beta$. Then

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z}, \tag{17}$$

$n = 1, 2, 3, \dots$, is a divisibility sequence. Indeed, if $r|s$ then, setting $l := s/r \in \mathbb{N}$, we see that

$$\frac{u_s}{u_r} = \frac{\alpha^{rl} - \beta^{rl}}{\alpha^r - \beta^r} = \alpha^{r(l-1)} + \alpha^{r(l-2)}\beta^r + \cdots + \beta^{r(l-1)}$$

is a symmetric function in α, β. Hence $u_s/u_r \in \mathbb{Z}$, giving $u_r | u_s$. If $(x_n)_{n=1}^{\infty}$ is a sequence given by the linear recurrence (1) then one can consider a corresponding divisibility sequence, by selecting $u_1 := 1$, $u_2 := a$. This sequence is called the *Lucas sequence of the first kind*.

From (1) and (17) one can calculate the terms of the Lucas sequence as follows

$$u_3 = au_2 + bu_1 = a^2 + b,$$
$$u_4 = au_3 + bu_2 = a\big(a^2 + b\big) + ba = a\big(a^2 + 2b\big),$$
$$u_6 = u_3\big(\alpha^3 + \beta^3\big) = u_3\big((\alpha+\beta)^3 - 3\alpha\beta(\alpha+\beta)\big) = a\big(a^2 + b\big)\big(a^2 + 3b\big),$$
$$u_{12} = u_6\big(\alpha^6 + \beta^6\big) = u_6\big(\big(\alpha^3 + \beta^3\big)^2 - 2(\alpha\beta)^3\big) = a\big(a^2 + b\big)\big(a^2 + 2b\big)\big(a^2 + 3b\big)\big(a^4 + 4a^2b + b^2\big).$$

To obtain the last equality we used the identity

$$\big(a\big(a^2 + 3b\big)\big)^2 + 2b^3 = \big(a^2 + 2b\big)\big(a^4 + 4a^2b + b^2\big).$$

Lemma 8. *If $b = -1$ and $|a| \geqslant 4$ then there exist five distinct prime numbers p_i, $i = 1, \ldots, 5$, such that $p_1|u_2$, $p_2|u_3$, $p_3|u_4$, $p_4|u_6$ and $p_5|u_{12}$.*

Proof. Let p_1 be any prime divisor of $u_2 = a$, and let $p_2 \neq 2$ be any prime divisor of $u_3 = a^2 - 1 = (a-1)(a+1)$. Such p_2 exists, because $|a| \geqslant 4$. Clearly, $p_2 \neq p_1$. Since $a^2 - 2$ is either 2 or 3 modulo 4, it is not divisible by 4. So $a^2 - 2$ must have an odd prime divisor p_3. Clearly, $p_3 \neq p_1$. Furthermore, $p_3 \neq p_2$, because $\gcd(a^2 - 1, a^2 - 2) = 1$. We select this p_3 as a divisor of u_4. Observing that 9 does not divide $a^2 - 3$, we get that there is prime number $p_4 \neq 3$ that divides $a^2 - 3$. Since $\gcd(a, a^2 - 3)$ is either 1 or 3, this yields $p_4 \neq p_1$. Also, since $\gcd(a^2 - 1, a^2 - 3)$ is either 1 or 2, we may have $p_4 = p_2$ only if $p_2 = 2$, which is not the case. So $p_4 \neq p_2$. The fact that $p_4 \neq p_3$ follows from $\gcd(a^2 - 2, a^2 - 3) = 1$. We select this p_4 as a divisor of u_6.

It remains to show that there is a prime divisor p_5 of $a^4 - 4a^2 + 1$ distinct from p_i, $i = 1, \ldots, 4$. Note that $a^4 - 4a^2 + 1$ is not zero modulo 4 and modulo 3. Hence there is a prime number $p_5 \neq 2, 3$ that divides $a^4 - 4a^2 + 1 \geqslant 4^4 - 4^3 + 1 = 193$. Evidently, $p_5 \neq p_1$. Writing

$$a^4 - 4a^2 + 1 = \big(a^2 - 1\big)\big(a^2 - 3\big) - 2$$

and using $p_5 \neq 2$, we may conclude that $p_5 \neq p_2, p_4$. Similarly, from $a^4 - 4a^2 + 1 = (a^2 - 2)^2 - 3$ and $p_5 \neq 3$, we see that $p_5 \neq p_3$. □

One can easily check that Lemma 8 does not hold for $|a| = 3$. The next lemma is very similar to that above.

Lemma 9. *If $b = 1$ and $|a| \geqslant 2$ then there exist five distinct prime numbers p_i, $i = 1, \ldots, 5$, such that $p_1|u_2$, $p_2|u_3$, $p_3|u_4$, $p_4|u_6$ and $p_5|u_{12}$.*

Proof. Take any prime divisor p_1 of $u_2 = a$. Let $p_2 \neq 2$ be any prime divisor of $u_3 = a^2 + 1$. Such p_2 exists, because $a^2 + 1$ is not divisible by 4. Evidently, $p_2 \neq p_1$. Similarly, let $p_3 \neq 2$ be any prime divisor of $a^2 + 2$. Clearly, $p_3 \neq p_2$. Since $\gcd(a, a^2 + 2)$ is either 1 or 2, $p_3 = p_1$ only if they both are equal to 2, which is not the case. So we may select this p_3 as a divisor of u_4. Observing next that 9 does not divide $a^2 + 3$, we deduce that there is prime number $p_4 \neq 3$ that divides $a^2 + 3$. Since $\gcd(a, a^2 + 3)$ is either 1 or 3, this yields $p_4 \neq p_1$. Also, since $\gcd(a^2 + 1, a^2 + 3)$ is either 1 or 2, we may have $p_4 = p_2$ only if $p_2 = 2$, which is not the case. Hence $p_4 \neq p_2$. As above, the fact that $p_4 \neq p_3$ follows from $\gcd(a^2 + 2, a^2 + 3) = 1$. We select this p_4 as a divisor of u_6.

It remains to show that there is a prime divisor p_5 of $a^4 + 4a^2 + 1$ which is distinct from p_i, $i = 1, \ldots, 4$. Note that $a^4 + 4a^2 + 1 > 6$ is not zero modulo 4 and modulo 9. Hence there is a prime $p_5 \neq 2, 3$ that divides $a^4 + 4a^2 + 1$. Evidently, $p_5 \neq p_1$. Writing

$$a^4 + 4a^2 + 1 = \big(a^2 + 1\big)\big(a^2 + 3\big) - 2$$

and using $p_5 \neq 2$, we may conclude that $p_5 \neq p_2, p_4$. Finally, from $a^4 + 4a^2 + 1 = (a^2 + 2)^2 - 3$ and $p_5 \neq 3$, it follows that $p_5 \neq p_3$. □

To illustrate Lemma 9, let us take $(a, b) = (\pm 2, 1)$. Then $u_2 = \pm 2$, $u_3 = 5$, $u_4 = \pm 2^2 \cdot 3$, $u_6 = \pm 2 \cdot 5 \cdot 7$ and $u_{12} = \pm 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. Hence Lemma 9 holds with $p_1 = 2$, $p_2 = 5$, $p_3 = 3$, $p_4 = 7$, $p_5 = 11$.

The next lemma uses the concept of covering systems introduced by Erdős. A collection of residue classes

$$r_i \pmod{m_i} := \{r_i + m_i k \mid k \in \mathbb{Z}\},$$

where $m_i \in \mathbb{N}$, $r_i \in \mathbb{Z}$, $0 \leqslant r_i < m_i$, and $i = 1, \ldots, t$, is called a *covering system* if every integer $n \in \mathbb{Z}$ belongs to at least one residue class $r_i \pmod{m_i}$, where $1 \leqslant i \leqslant t$. In the proof of the theorem for $|b| = 1$ we shall use the following well-known covering system

$$0 \pmod 2, \qquad 0 \pmod 3, \qquad 1 \pmod 4, \qquad 5 \pmod 6, \qquad 7 \pmod{12}. \tag{18}$$

Lemma 10. *Let $r_i \pmod{m_i}$, $i = 1, \ldots, t$, be a covering system, and let $(u_n)_{n=1}^{\infty}$ be a divisibility sequence given by $u_1 := 1$, $u_2 := a$ and $u_{n+1} = au_n + bu_{n-1}$ for $n = 2, 3, \ldots$, where $a \in \mathbb{Z}$, $b = \pm 1$ and $D = a^2 + 4b > 0$. Suppose that there exist t distinct prime numbers $p_1, \ldots, p_t$ such that $p_i | u_{m_i}$ for each $i = 1, \ldots, t$. Then there are two relatively prime composite positive integers x_1, x_2 such that each $|x_n|$, $n \in \mathbb{N}$, where x_n is a sequence defined in* (1)*, is a composite number.*

Proof. By the Chinese remainder theorem, there exist $s, l \in \mathbb{Z}$ satisfying

$$s \equiv u_{m_i - r_i} \pmod{p_i},$$
$$l \equiv u_{m_i - r_i + 1} \pmod{p_i}$$

for $i = 1, \ldots, t$. Note that two consecutive terms of the sequence $(u_n)_{n=1}^{\infty}$ cannot be divisible by the same prime number p. Indeed, if $p | u_n$ and $p | u_{n+1}$ then using $b = \pm 1$ from $u_{n+1} = au_n + bu_{n-1}$ we find that $p | u_{n-1}$. By the same argument, $p | u_{n-2}$ and so on. Hence $p | u_1$, a contradiction.

So, for every x_1 in the residue class $s \pmod P$, where $P = p_1 \ldots p_t$, and for every x_2 in the residue class $l \pmod P$, we have $x_1 \equiv u_{m_i - r_i} \pmod{p_i}$ and $x_2 \equiv u_{m_i - r_i + 1} \pmod{p_i}$ for $i = 1, \ldots, t$. By induction on n, this implies

$$x_{n+1} \equiv u_{m_i - r_i + n} \pmod{p_i} \tag{19}$$

for each $n \geqslant 0$ and each $i = 1, \ldots, t$. Since $r_i \pmod{m_i}$, $i = 1, \ldots, t$, is a covering system, every non-negative integer n belongs to certain residue class $r_i \pmod{m_i}$, where i is some of the numbers $1, \ldots, t$. Fix one of those i and write $n = r_i + km_i$, where $k \geqslant 0$. Note that $p_i | u_{m_i(k+1)}$, because $p_i | u_{m_i}$ and $u_{m_i} | u_{m_i(k+1)}$. Thus (19) yields

$$x_{n+1} \equiv u_{m_i(k+1)} \pmod{p_i} \equiv 0 \pmod{p_i},$$

giving $p_i | x_{n+1}$.

It remains to choose two composite relatively prime positive integers $x_1 \equiv s \pmod P$ and $x_2 \equiv l \pmod P$ so that $|x_n| > \max(p_1, \ldots, p_t)$ for every $n \in \mathbb{N}$. Then each $|x_n|$ is divisible by some p_i and greater than p_i, so it is a composite number. To do this let us choose a composite integer $x_1 > \max(p_1, \ldots, p_t)$ satisfying $x_1 \equiv s \pmod P$. Then we can select $x_2 \equiv l \pmod P$ as required, by

Lemmas 6 and 7, where $a_1 := l$, $b_1 := P$, $b_2 := x_1$, because no prime number $p_1, \dots, p_t$ divides both s and l. $\square$

Now, we shall prove the theorem for $|b| = 1$. Suppose first that $b = -1$ and $|a| \geqslant 4$. Then, by Lemma 8, there are five distinct primes $p_1, \dots, p_5$ dividing $u_2, u_3, u_4, u_6, u_{12}$, respectively. Since $D = a^2 - 4 > 0$, the theorem follows from Lemma 10 applied to the covering system (18). Similarly, if $b = 1$ and $|a| \geqslant 2$ we also have $D = a^2 + 4b = a^2 + 4 > 0$, so the theorem follows by Lemmas 9 and 10.

Recall that the cases $b = -1$, $|a| \leqslant 2$ and $b = 1$, $a = 0$ have been considered in Section 2. In Section 1 we already described the literature concerning the case $(a, b) = (1, 1)$. So three cases that remain to be considered are $(a, b) = (-1, 1)$, $(a, b) = (-3, -1)$, $(a, b) = (3, -1)$.

We begin with the case $(a, b) = (-1, 1)$. Vsemirnov's pair (2) of two composite relatively prime integers

$$V_1 := 106276436867, \qquad V_2 := 35256392432$$

shows that the numbers

$$V_n = V_{n-1} + V_{n-2} = F_{n-1}V_2 + F_{n-2}V_1, \quad n \geqslant 2, \tag{20}$$

are all composite. Here, F_n is the nth Fibonacci number, $F_0 := 0$. For the sequence $x_{n+1} = -x_n + x_{n-1}$, we clearly have

$$x_n = (-1)^n F_{n-1}x_2 + (-1)^{n-1} F_{n-2}x_1, \quad n \geqslant 3. \tag{21}$$

Selecting $x_1 := -V_2 + V_1 = 71020044435$ and $x_2 := V_1 = 106276436867$, one can easily check that x_1 and x_2 are relatively prime composite integers. Moreover, by (20) and (21),

$$\begin{aligned} x_n &= (-1)^n F_{n-1}V_1 + (-1)^{n-1} F_{n-2}(-V_2 + V_1) = (-1)^n F_{n-2}V_2 + (-1)^n F_{n-3}V_1 \\ &= (-1)^n (F_{n-2}V_2 + F_{n-3}V_1) = (-1)^n V_{n-1} \end{aligned}$$

for $n \geqslant 3$. Thus $|x_n| = V_{n-1}$ is also composite integer for each $n \geqslant 3$.

For $(a, b) = (-3, -1)$, we use the covering system

$$\begin{gathered} 1 \pmod 2, \qquad 1 \pmod 3, \qquad 0 \pmod 4, \\ 6 \pmod 8, \qquad 6 \pmod{12}, \qquad 2 \pmod{24}. \end{gathered}$$

The divisibility sequence $(u_n)_{n=1}^{\infty}$ is given by $u_1 := 1$, $u_2 := -3$ and $u_{n+1} = -3u_n - u_{n-1}$, $n = 2, 3, \dots$. We select the following primes dividing $u_2, u_3, u_4, u_8, u_{12}, u_{24}$, respectively: $3, 2, 7, 47, 23, 1103$. By the method described in Lemma 10, we calculated the pair

$$(x_1, x_2) = (13271293, 219498)$$

satisfying the conditions of the theorem.

For $(a, b) = (3, -1)$, we use the covering system

$$\begin{gathered} 0 \pmod 2, \qquad 0 \pmod 3, \qquad 3 \pmod 4, \\ 5 \pmod 8, \qquad 5 \pmod{12}, \qquad 1 \pmod{24}. \end{gathered}$$

As above, the primes dividing $u_2, u_3, u_4, u_8, u_{12}, u_{24}$ are $3, 2, 7, 47, 23, 1103$, respectively. This time, using the method described in Lemma 10, we found the pair

$$(x_1, x_2) = (7373556, 2006357)$$

satisfying the conditions of the theorem. The proof of Theorem 1 is thus completed.

Below, we shall find smaller solutions for $(a, b) = (\pm 3, -1)$. Instead of using Lemma 10, we may directly search for a pair of relatively prime positive integers x_1, x_2 such that each of the first 24 elements of the sequence (1) is divisible by at least one of the primes $3, 2, 7, 47, 23, 1103$. Then we may choose a covering system $r_i \pmod{m_i}$, where $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $m_4 = 8$, $m_5 = 12$, $m_6 = 24$, and $i = 1, \ldots, 6$, such that, for each n in the range $0 \leqslant n \leqslant 23$ and each i in the range $1 \leqslant i \leqslant 6$, $n + 1 \equiv r_i \pmod{m_i}$ implies $p_i | x_{n+1}$. This would be enough for $p_i | x_{n+1}$ to hold for any $n + 1$, $n \geqslant 0$, belonging to the residue class $r_i \pmod{m_i}$. Using this direct method, we found smaller pairs (x_1, x_2) producing sequences consisting of composite numbers.

For $(a, b) = (-3, -1)$, by selecting the residues of the covering system as

$$(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 1, 0, 2, 6, 14)$$

and searching over x_1 divisible by 7 and x_2 divisible by 2 and 3, we found the pair

$$(x_1, x_2) = (35, 3294).$$

One can easily check that

$$1 \pmod 2, \qquad 1 \pmod 3, \qquad 0 \pmod 4,$$

$$2 \pmod 8, \qquad 6 \pmod{12}, \qquad 14 \pmod{24}$$

is indeed a covering system. Also, if $n + 1$, where $n \geqslant 0$, belongs to the residue class $r_i \pmod{m_i}$ we use the fact that $p_i | x_{n+1}$. This explains why we take x_1 divisible by 7 and x_2 divisible by 6. It is clear that $\gcd(x_1, x_2) = \gcd(35, 3294) = 1$. Also, $|x_n| > \max(p_1, \ldots, p_6) = 1103$ for $n \geqslant 2$, so $|x_n|$ is composite for each $n \in \mathbb{N}$.

Selecting $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 0, 1, 7, 7, 11)$, we found the symmetric pair $(x_1, x_2) = (3294, 35)$. Similarly, taking $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 2, 1, 3, 3, 7)$, we established that

$$(x_1, x_2) = (2367, 3031)$$

is also such a pair. Note that $3294 + 35 < 2367 + 3031$. On the other hand, $\max(3294, 35) > \max(2367, 3031)$. In the same way, using $(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 2, 0, 6, 10, 18)$, we found the symmetric pair $(x_1, x_2) = (3031, 2367)$.

For $(a, b) = (3, -1)$, selecting $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 2, 1, 3, 7, 15)$, we found the pair

$$(x_1, x_2) = (3399, 35).$$

Choosing the residues $(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 2, 0, 6, 6, 10)$, we arrived to the symmetric pair $(x_1, x_2) = (35, 3399)$.

References

[1] G. Alkauskas, A. Dubickas, Prime and composite numbers as integer parts of powers, Acta Math. Hungar. 105 (2004) 249–256.
[2] R.C. Baker, G. Harman, Primes of the form $[c^p]$, Math. Z. 221 (1996) 73–81.
[3] A. Dubickas, A. Novikas, Integer parts of powers of rational numbers, Math. Z. 251 (2005) 635–648.
[4] W. Forman, H.N. Shapiro, An arithmetic property of certain rational powers, Comm. Pure Appl. Math. 20 (1967) 561–573.
[5] R.L. Graham, A Fibonacci-like sequence of composite numbers, Math. Mag. 37 (1964) 322–324.
[6] R.K. Guy, Unsolved Problems in Number Theory, Springer-Verlag, New York, 1994.
[7] M. Hall, Divisibility sequences of third order, Amer. J. Math. 58 (1936) 577–584.
[8] D.E. Knuth, A Fibonacci-like sequence of composite numbers, Math. Mag. 63 (1990) 21–25.
[9] J.W. Nicol, A Fibonacci-like sequence of composite numbers, Electron. J. Combin. 6 (1999), #R44, 6 p.
[10] M. Vsemirnov, A new Fibonacci-like sequence of composite numbers, J. Integer Seq. 7 (2004), Article 04.3.7, 3 p.
[11] H.S. Wilf, Letters to the editor, Math. Mag. 63 (1990) 284.